

## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of activating a smart card, comprising:
  - receiving identifying information for a non-activated smart card that is being used for the first time by a user;
  - receiving manual authentication information for the user to whom the non-activated smart card has been issued;
  - authenticating the user and the non-activated smart card using the identifying information and the manual authentication information;
  - obtaining a public key from the non-activated smart card; and
  - issuing a digital certificate that is generated using the public key,wherein the non-activated smart card is activated upon receiving the digital certificate.
2. (Previously Amended) The method according to claim 1, wherein the manual authentication information comprises a user identifier and a password.
3. (Original) The method according to claim 1, further comprising obtaining the digital certificate from a certificate authority.
4. (Previously Amended) The method according to claim 1, wherein the smart card is connected to a workstation.
5. (Previously Amended) The method according to claim 1, wherein the digital certificate is stored in at least one of the activated smart

card and a workstation.

6. (Previously Amended) The method according to claim 1, further comprising:

receiving a login request that is initiated when the activated smart card is connected to a workstation;

authenticating the activated smart card using the digital certificate; and

if authenticated, permitting a login to a computer resource.

7. (Previously Amended) The method according to claim 6, wherein the activated smart card is removed from the workstation after it is authenticated.

8. (Previously Amended) The method according to claim 6, wherein authenticating the activated smart card further comprises determining that the digital certificate has not been revoked.

9. (Currently Amended) A method of activating a smart card, comprising:

sending, to an administration server, identifying information read from a non-activated smart card that has not been previously used by a user to whom the non-activated smart card has been issued;

sending, to the administration server, manual authentication information input by a the user ~~to whom the non-activated smart card has been issued;~~

generating a public key using the non-activated smart card;  
sending the public key to the administration server; and  
receiving a digital certificate that is generated using the public key,  
wherein the non-activated smart card is activated upon receipt of the digital certificate.

10. (Previously Amended) The method according to claim 9,  
wherein the manual authentication information comprises a user  
identifier and a password.

11. (Original) The method according to claim 9, further  
comprising receiving the digital certificate from a certificate authority.

12. (Previously Amended) The method according to claim 9,  
wherein the smart card is connected to a workstation.

13. (Previously Amended) The method according to claim 9,  
further comprising storing the digital certificate in at least one of the  
activated smart card and a workstation.

14. (Previously Amended) The method according to claim 9,  
further comprising:

connecting the activated smart card to a workstation;  
sending a login request to a server that authenticates the digital  
certificate against a certificate revocation list; and  
if authenticated, permitting a login to a computer resource.

15. (Previously Amended) The method according to claim 14, wherein the activated smart card is removed from the workstation after the digital certificate is sent.

16. (Previously Amended) The method according to claim 14, wherein the server determines that the digital certificate has not been revoked.

Claims 17-22 (Canceled).

23. (Currently Amended) A method of activating a smart card then using a an activated smart card, comprising:

on first use of ~~the~~ a non-activated smart card by a user to whom the non-activated smart card has been issued:

receiving identifying information for ~~a~~ the non-activated smart card;

receiving manual identification information for ~~a~~ the user ~~to whom the non-activated smart card has been issued~~;

authenticating the user and the non-activated smart card using the manual authentication information and the identifying information;

obtaining a public key from the non-activated smart card; and  
sending a digital certificate generated using the public key from a certificate authority to the non-activated smart card, wherein the non-activated smart card is activated upon receiving the digital

certificate; and

on a subsequent use of the smart card:

receiving a login request that is initiated when the activated smart card is connected to a workstation;

authenticating the digital certificate against a certificate revocation list to determine that the digital certificate has not been revoked; and

if authenticated, permitting a login to a computer resource.

24. (Previously Amended) The method according to claim 23, wherein the activated smart card is connected to a workstation and removed from the workstation after it is authenticated.

25. (Previously Amended) The method according to claim 23, wherein the digital certificate is stored in at least one of the activated smart card and a workstation.